Begrijp Nexus VPC Loop Avoidance

Inhoud

Inleiding

In dit document worden scenario's beschreven waarin het vermijden van vPC-loops van invloed kan zijn op het doorsturen van verkeer in op Nexus gebaseerde Layer 3-netwerkontwerpen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CLI voor Nexus-besturingssysteem
- vPC-concepten

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Software 10.4(4)

- Hardware N9K-C9364C-GX

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

In de huidige datacenteromgevingen is de Cisco Nexus Virtual Port Channel (vPC)-technologie van essentieel belang om redundantie en taakverdeling mogelijk te maken. Door het mogelijk te maken dat aansluitingen op twee aparte Nexus-switches als één logisch poortkanaal functioneren, vereenvoudigt vPC de netwerkarchitectuur en verbetert het de betrouwbaarheid van downstreamapparaten. Bepaalde configuratiedetails kunnen echter operationele complexiteit met zich meebrengen.

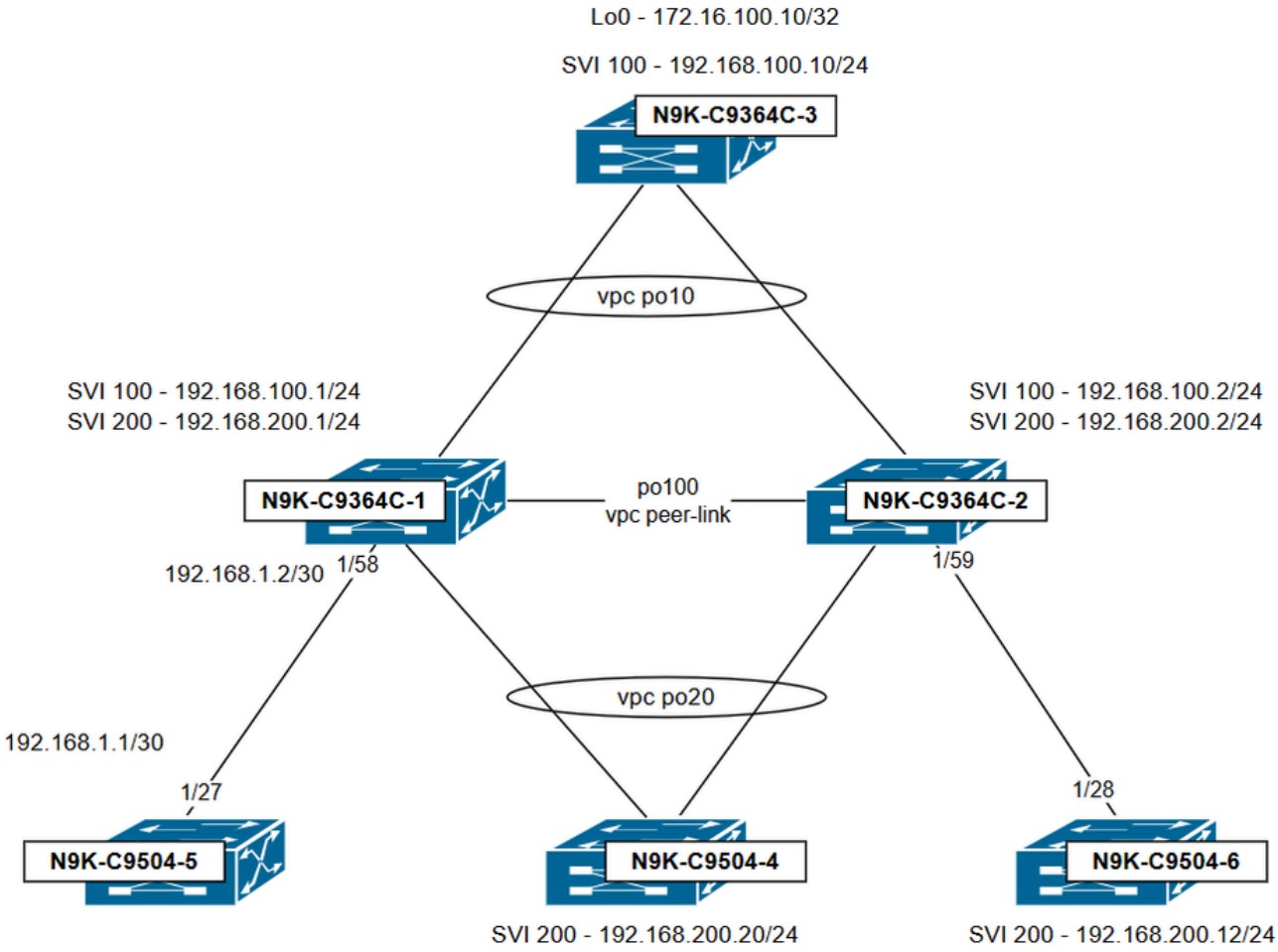
In dit document worden scenario's onderzocht waarin vPC Loop Avoidance significant wordt en wordt de impact ervan op het doorsturen van verkeer onderzocht. Een duidelijk begrip van dit mechanisme is van cruciaal belang voor netwerkingenieurs die robuuste, efficiënte Layer 3-connectiviteit willen ontwerpen en onderhouden in een op Nexus gebaseerde infrastructuur, waardoor verkeersverstoringen worden voorkomen en optimale netwerkprestaties worden behouden.

Probleem

In een Cisco Nexus-omgeving die vPC gebruikt, kunnen netwerkbeheerders onverwacht doorstuurgedrag van het verkeer observeren dat wordt veroorzaakt door de regel voor het vermijden van vPC-lus. Wanneer verkeer van de ene vPC-peer naar de andere gaat via de vPC-peer-link, kan het niet worden afgesloten via een vPC-poortkanaal dat op beide switches actief is. Als gevolg hiervan kunnen apparaten die afhankelijk zijn van dit pad voor connectiviteit pakketten laten vallen of connectiviteitsverlies ervaren, zelfs als alle fysieke links omhoog lijken te zijn.

Inzicht in en verantwoording voor de vPC-lusvermijdingsregel is essentieel voor het ontwerpen en oplossen van problemen met veerkrachtige netwerktopologieën, omdat het negeren van dit gedrag kan leiden tot onverwachte serviceonderbrekingen en netwerkproblemen moeilijker te diagnosticeren kan maken.

Netwerkdiagram



In deze topologie wordt het vPC-domein gemaakt door N9K-C9364C-1 en N9K-C9364C-2. Beide switches zijn geconfigureerd met VLAN's 100 en 200 als vPC-VLAN's en SVI's zijn ingesteld voor elk VLAN. Het vPC-domein is verantwoordelijk voor inter-VLAN-routering tussen deze VLAN's. Tenzij anders aangegeven, wordt de HSRP virtual IP (VIP) gedeeld tussen de vPC peer-switches gebruikt als de volgende stap voor de standaardroute door de andere switches in de topologie.

- N9K-C9364C-1 SVI-configuratie

interface VLAN100
Geen afsluiting
no ip redirects
IP-adres 192.168.100.1/24
Geen IPv6-omleidingen
HRP 100
IP 192 168 100 254

interface VLAN200
Geen afsluiting
no ip redirects
IP-adres 192.168.200.1/24
Geen IPv6-omleidingen

HRP 200
IP 192 168 200 254

- N9K-C9364C-2 SVI-configuratie

interface VLAN100
Geen afsluiting
no ip redirects
IP-adres 192.168.100.2/24
Geen IPv6-omleidingen
HRP 100
IP 192 168 100 254

interface VLAN200
no ip redirects
IP-adres 192.168.200.2/24
Geen IPv6-omleidingen
HRP 200
IP 192 168 200 254

Scenario's

Scenario 1: SVI voor vPC VLAN wordt administratief afgesloten op vPC Peer

a) Gerouteerd verkeer van vPC naar vPC wordt beïnvloed

In een werkscenario kan N9K-C9504-4 (VLAN 200) met succes Ping N9K-C9364C-3 (VLAN 100). Traceroute geeft aan dat het verbindingspad loopt door 192.168.200.2, dat is toegewezen aan N9K-C9364C-2.

<#root>

```
N9K-C9504-4#
```

ping 192.168.100.10

```
PING 192.168.100.10 (192.168.100.10): 56 data bytes
64 bytes from 192.168.100.10: icmp_seq=0 ttl=253 time=8.48 ms
64 bytes from 192.168.100.10: icmp_seq=1 ttl=253 time=0.618 ms
64 bytes from 192.168.100.10: icmp_seq=2 ttl=253 time=0.582 ms
64 bytes from 192.168.100.10: icmp_seq=3 ttl=253 time=0.567 ms
64 bytes from 192.168.100.10: icmp_seq=4 ttl=253 time=0.55 ms

--- 192.168.100.10 ping statistics ---
```

5 packets transmitted, 5 packets received, 0.00% packet loss

```
round-trip min/avg/max = 0.55/2.159/8.48 ms
N9K-C9504-4#
```

```
<#root>

N9K-C9504-4#

traceroute 192.168.100.10


traceroute to 192.168.100.10 (192.168.100.10), 30 hops max, 40 byte packets

1 192.168.200.2 (192.168.200.2) 1.129 ms 0.602 ms 0.724 ms    <<<---- SVI 200 on N9K-C9364C-2


2 192.168.100.10 (192.168.100.10) 1.001 ms 0.657 ms 0.588 ms
```

Op dit punt werkt de verkeersstroom op deze manier:

- N9K-C9364C-2 ontvangt verkeer vanaf 192.168.200.20 bestemd voor 192.168.100.10, waarbij het MAC-adres van de bestemming is ingesteld op de gedeelde HSRP Virtual MAC (VMAC) binnen het vPC-domein.
- Omdat HSRP in de Active-Active-modus werkt vanuit een data plane-perspectief op de vPC, routeert N9K-C9364C-2 het verkeer van VLAN 200 naar VLAN 100 en stuurt het door naar vPC 10.

Overweeg een scenario waarbij SVI 200 is uitgeschakeld op N9K-C9364C-2, maar actief blijft op N9K-C9364C-1:

```
<#root>

N9K-C9364C-1#

show ip interface brief


IP Interface Status for VRF "default"(1)
Interface IP Address Interface Status
Vlan100 192.168.100.1 protocol-up/link-up/admin-up

Vlan200 192.168.200.1 protocol-up/link-up/admin-up <<<---- SVI 200 is up


N9K-C9364C-1#
```

```
<#root>

N9K-C9364C-2#

show ip interface brief


IP Interface Status for VRF "default"(1)
Interface IP Address Interface Status
Vlan100 192.168.100.2 protocol-up/link-up/admin-up
```

```
Vlan200 192.168.200.2 protocol-down/link-down/admin-down  <<<---- SVI 200 is down

N9K-C9364C-2#
```

Vanwege het verschil in operationele status van de SVI's tussen de vPC-peers, wordt een type 2-inconsistentie gedetecteerd binnen het vPC-domein:

<#root>

```
N9K-C9364C-1#

show vPC


Legend:
(*) - local vPC is down, forwarding via vPC peer-link

vPC domain id : 100
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : failed

Type-2 inconsistency reason : SVI type-2 configuration incompatible


vPC role : primary
Number of vPCs configured : 2
Peer Gateway : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Disabled
Delay-restore status : Timer is off.(timeout = 30s)
Delay-restore SVI status : Timer is off.(timeout = 10s)
Delay-restore Orphan-port status : Timer is off.(timeout = 0s)
Operational Layer3 Peer-router : Disabled
Virtual-peerlink mode : Disabled

vPC Peer-link status
---------------------------------------------------------------------
id Port Status Active vlans
-- ---- ------ --------------------------------------------------
1 Po100 up 1,100,200

vPC status
----------------------------------------------------------------------------
Id Port Status Consistency Reason Active vlans
-- ------------ ------ ----------- ------ ---------------
10 Po10 up success success 1,100,200
20 Po20 up success success 1,100,200
N9K-C9364C-1#
```

<#root>

```
N9K-C9364C-2#
```

```
show vPC


Legend:
(*) - local vPC is down, forwarding via vPC peer-link

vPC domain id : 100
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : failed

Type-2 inconsistency reason : SVI type-2 configuration incompatible


vPC role : secondary
Number of vPCs configured : 2
Peer Gateway : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Disabled
Delay-restore status : Timer is off.(timeout = 30s)
Delay-restore SVI status : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router : Disabled
Virtual-peerlink mode : Disabled

vPC Peer-link status
---------------------------------------------------------------------
id Port Status Active vlans
-- ---- ------ --------------------------------------------------
1 Po100 up 1,100,200

vPC status
----------------------------------------------------------------------------
Id Port Status Consistency Reason Active vlans
-- ------------ ------ ----------- ------ ---------------
10 Po10 up success success 1,100,200
20 Po20 up success success 1,100,200

N9K-C9364C-2#
```

In dit stadium is het verkeer van 192.168.200.20 tot 192.168.100.10 niet langer succesvol:

<#root>

```
N9K-C9504-4#

ping 192.168.100.10


PING 192.168.100.10 (192.168.100.10): 56 data bytes
Request 0 timed out
Request 1 timed out
Request 2 timed out
Request 3 timed out
Request 4 timed out

--- 192.168.100.10 ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss
```

```
N9K-C9504-4#
```

Een gekleurde ping (een ping met een opgegeven MTU-grootte) wordt gebruikt om het pad te traceren dat door dit verkeer wordt genomen:

<#root>

```
N9K-C9504-4#

ping 192.168.100.10 count 100 timeout 0 packet-size 1030


PING 192.168.100.10 (192.168.100.10): 1030 data bytes
Request 0 timed out
Request 1 timed out
---- snip -----
Request 98 timed out
Request 99 timed out

--- 192.168.100.10 ping statistics ---

100 packets transmitted, 0 packets received, 100.00% packet loss


N9K-C9504-4# ^C
N9K-C9504-4#
```

Volgens de interfacetellers op N9K-C9364C-2 wordt dit verkeer ontvangen op poortkanaal 20 en doorgestuurd naar poortkanaal 100 (de vPC-peer-link):

<#root>

```
N9K-C9364C-2#

show interface port-channel 20 counters detailed all | i "1024 to|po" ; sh int port-channel 10 counters


port-channel20


52.

Rx Packets from 1024 to 1518 bytes: = 100    <<<----- Ingress vPC po20


60. Tx Packets from 1024 to 1518 bytes: = 0
port-channel10
52. Rx Packets from 1024 to 1518 bytes: = 0
60. Tx Packets from 1024 to 1518 bytes: = 0

port-channel100


52. Rx Packets from 1024 to 1518 bytes: = 0
60.
```

```
Tx Packets from 1024 to 1518 bytes: = 100 <<<----- Egress po100 (vPC peer-link)

N9K-C9364C-2#
```

Dit gedrag treedt op omdat SVI 200 is uitgeschakeld op N9K-C9364C-2, waardoor lokale routering van verkeer voor VLAN 200 wordt voorkomen. In dit scenario wordt het verkeer overbrugd over de vPC-peer-link naar N9K-C9364C-1, zodat dat apparaat de inter-VLAN-routering uitvoert.

Kijkend naar interfacetellers op N9K-C9364C-1, wordt bevestigd dat de pakketten dit apparaat bereiken via de vPC-peer-link, maar er zijn geen uitgaande pakketten waargenomen op vPC-poortkanaal 10, dat verbinding maakt met 192.168.100.10.

<#root>

```
N9K-C9364C-1#

show interface port-channel 20 counters detailed all | i "1024 to|po" ; sh int port-channel 10 counters


port-channel20
52. Rx Packets from 1024 to 1518 bytes: = 0
60. Tx Packets from 1024 to 1518 bytes: = 0
port-channel10
52. Rx Packets from 1024 to 1518 bytes: = 0
60.

Tx Packets from 1024 to 1518 bytes: = 0  <<<----- Expected egress vPC po10. No packets!!!


port-channel100
52.

Rx Packets from 1024 to 1518 bytes: = 100 <<<----- Ingress po100 (vPC peer-link)


60. Tx Packets from 1024 to 1518 bytes: = 0
N9K-C9364C-1#
```

Hoewel het verkeer op N9K-C9364C-1 aankomt via de vPC-peerlink, wordt het niet doorgestuurd naar vPC-poortkanaal 10. Dit komt omdat de egress_vsl_drop bit is ingesteld op 1 voor deze vPC, wat gebeurt wanneer hetzelfde vPC-poortkanaal werkt op de peer-switch (in dit geval N9K-C9364C-2).

<#root>

```
N9K-C9364C-1#

show system internal eltm info interface Po10 | i i vsl


egress_vsl_drop = 1
```

```
N9K-C9364C-1#
```

<#root>

```
N9K-C9364C-1#
```

show system internal vPCm info interface Po10 | i "Peer stat|Inform|vPC sta"

```
IF Elem Information:
MCECM DB Information:
```

vPC state: Up Old Compat Status: Pass

```
vPC Peer Information:
```

Peer state: Up   <<<------------- vPC 10 up on peer

```
PSS Information:
```

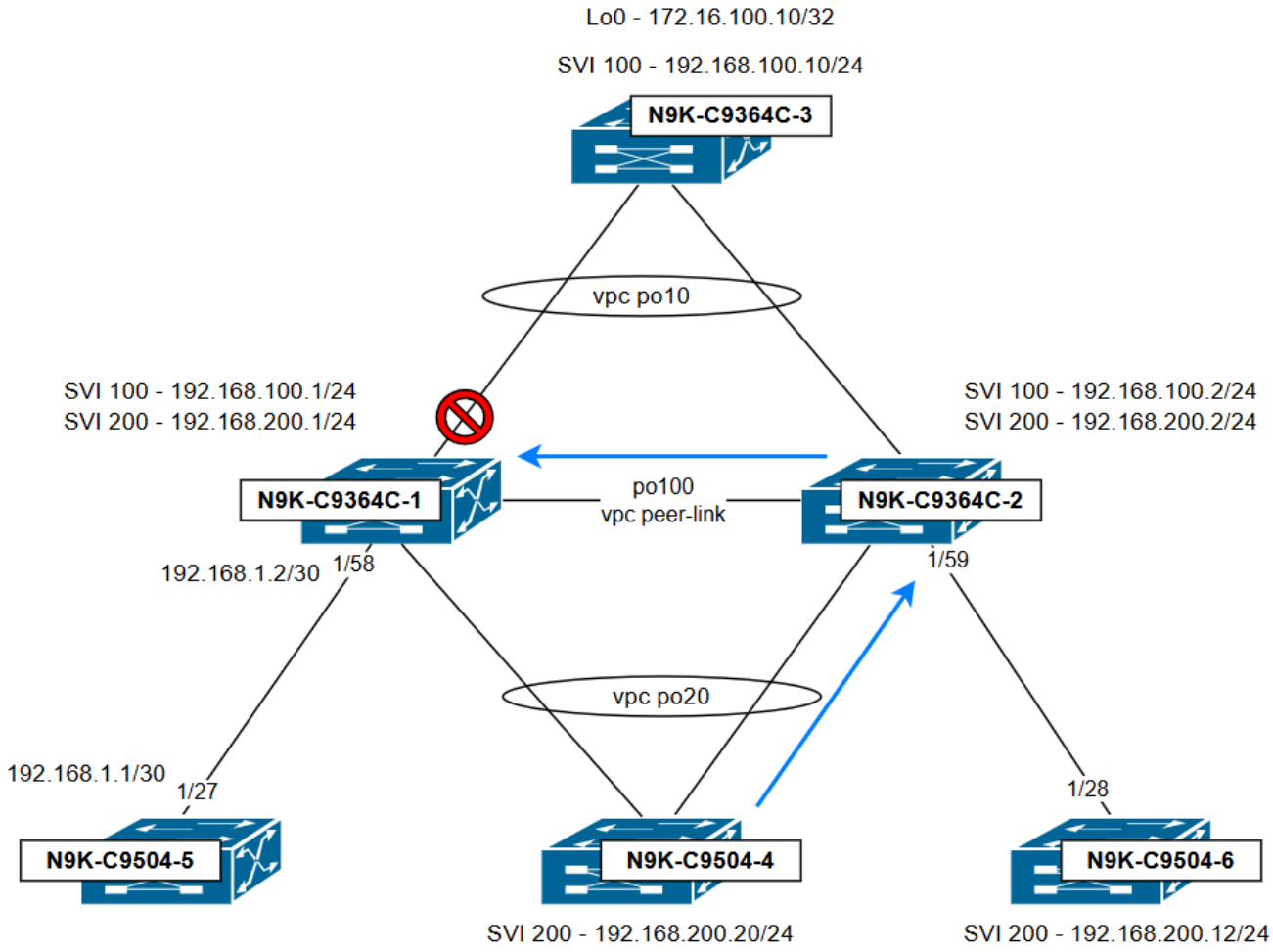
vPC state: Up Old Compat Status: Pass

```
vPC Peer Information:
```

Peer state: Up   <<<------------- vPC 10 up on peer

```
Shared Database Information:
Application database Information:
Lock Information:
N9K-C9364C-1#
```

Topologie ter illustratie van de verkeersstroom en het punt waarop deze wordt gedropt:



Conclusie:

N9K-C9364C-1 verlaagt het verkeer als gevolg van de vPC-lusvermijdingsregel: verkeer dat via de vPC-peer-link wordt ontvangen, kan niet worden doorgestuurd naar een vPC-poortkanaal dat op beide switches actief is."Om dit probleem te voorkomen, moet u ervoor zorgen dat de beheerstatus van de SVI's op beide switches consistent is en dat hun configuraties symmetrisch zijn.

b) Gerouteerd verkeer van weeshuis naar vPC-host wordt beïnvloed

Gezien hetzelfde scenario waarbij SVI 200 is uitgeschakeld op N9K-C9364C-2, maar actief blijft op N9K-C9364C-1. Een ping van N9K-C9504-6 (VLAN 200) naar N9K-C9364C-3 (VLAN 100) is mislukt.

<#root>

```
N9K-C9504-6#

ping 192.168.100.10 packet-size 1030 count 100 timeout 0


PING 192.168.100.10 (192.168.100.10): 1030 data bytes
Request 0 timed out
```

```
Request 1 timed out
Request 2 timed out
---- snip -----
Request 97 timed out
Request 98 timed out
Request 99 timed out

--- 192.168.100.10 ping statistics ---
100 packets transmitted, 0 packets received, 100.00% packet loss

N9K-C9504-6#
```

Een gekleurde ping (een ping met een opgegeven MTU-grootte) wordt gebruikt om het pad te traceren dat door dit verkeer wordt genomen:

<#root>

```
N9K-C9364C-2#
show interface eth1/59 counters detailed all | i "1024 to|Eth" ; sh int port-channel 10 counters detaile

Ethernet1/59
52. Rx Packets from 1024 to 1518 bytes: = 100 <<<----- Ingress port to N9K-C9504-6

60. Tx Packets from 1024 to 1518 bytes: = 0
port-channel10
52. Rx Packets from 1024 to 1518 bytes: = 0
60. Tx Packets from 1024 to 1518 bytes: = 0
port-channel100
52. Rx Packets from 1024 to 1518 bytes: = 0
60. Tx Packets from 1024 to 1518 bytes: = 100 <<<----- Egress po100 (vPC peer-link)

N9K-C9364C-2#
```

<#root>

```
N9K-C9364C-1#
show interface port-channel 10 counters detailed all | i "1024 to|po" ; sh int port-channel 100 counters

port-channel10
52. Rx Packets from 1024 to 1518 bytes: = 0
60. Tx Packets from 1024 to 1518 bytes: = 0 <<<----- Expected egress vPC po10. No packets!!!

port-channel100
52. Rx Packets from 1024 to 1518 bytes: = 100 <<<----- Ingress po100 (vPC peer-link)
```

```
60. Tx Packets from 1024 to 1518 bytes: = 0
N9K-C9364C-1#
```

Hoewel het verkeer op N9K-C9364C-1 aankomt via de vPC-peerlink, wordt het niet doorgestuurd naar vPC-poortkanaal 10. Dit komt omdat de egress_vsl_drop bit is ingesteld op 1 voor deze vPC, wat gebeurt wanneer hetzelfde vPC-poortkanaal werkt op de peer-switch (in dit geval N9K-C9364C-2).

<#root>

```
N9K-C9364C-1#
```

show system internal eltm info interface Po10 | i i vsl

egress_vsl_drop = 1

```
N9K-C9364C-1#
```

<#root>

```
N9K-C9364C-1#
```

show system internal vpcm info interface Po10 | i "Peer stat|Inform|vPC sta"

```
IF Elem Information:
MCECM DB Information:
```

vPC state: Up Old Compat Status: Pass

```
vPC Peer Information:
```

Peer state: Up <<<------------- vPC 10 up on peer

```
PSS Information:
```

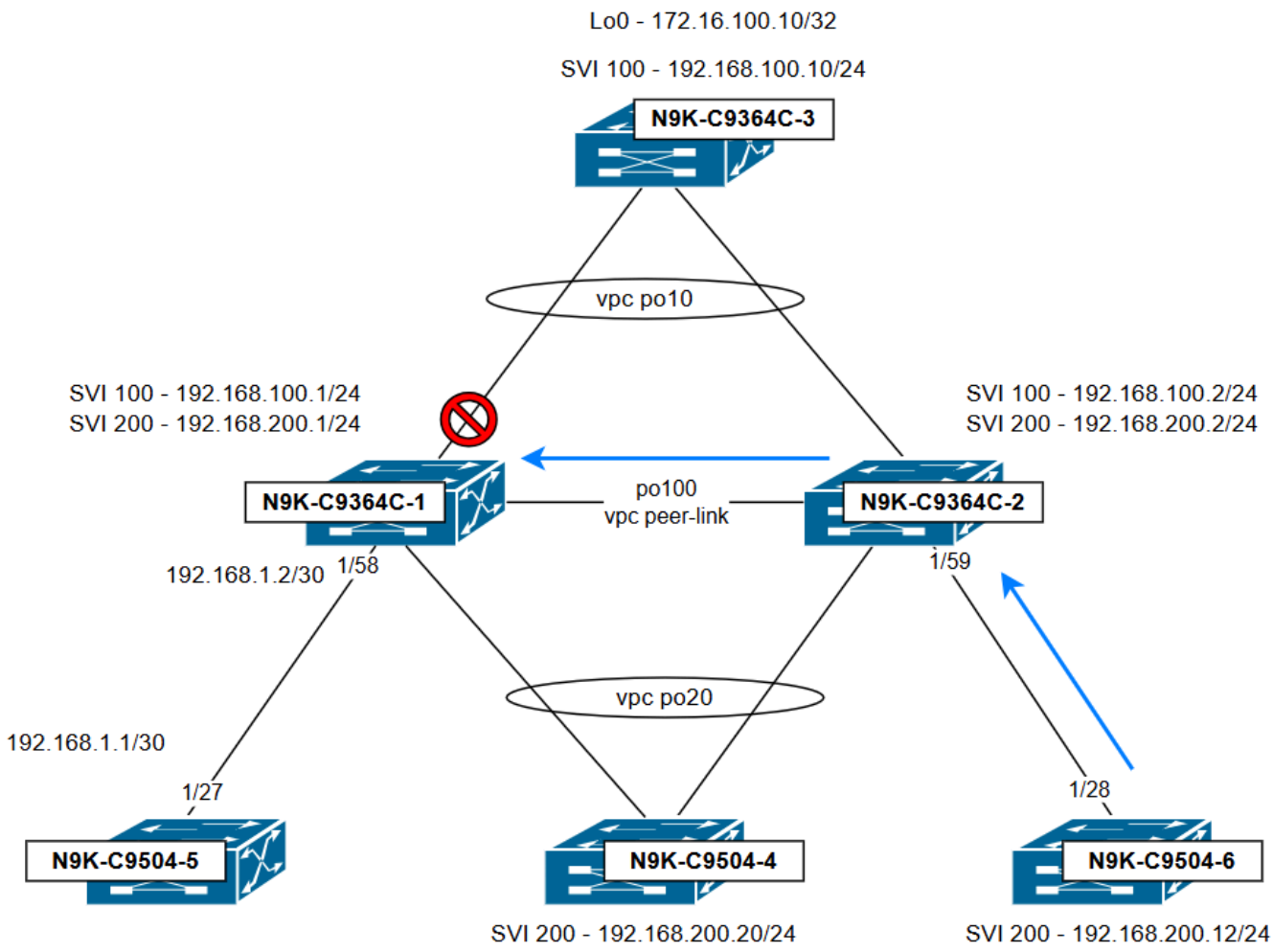
vPC state: Up Old Compat Status: Pass

```
vPC Peer Information:
```

Peer state: Up <<<------------- vPC 10 up on peer

```
Shared Database Information:
Application database Information:
Lock Information:
N9K-C9364C-1#
```

Topologie die de verkeersstroom en het punt waarop deze wordt gedropt illustreert:



Conclusie:

Hoewel het verkeer afkomstig is van een weeshost die is verbonden met N9K-C9364C-2, wordt het door N9K-C9364C-1 verwijderd vanwege de regel voor het vermijden van vPC-lus: verkeer dat via de vPC-peer-link wordt ontvangen, kan niet worden doorgestuurd naar een vPC-poortkanaal dat op beide switches actief is. Of de ingangspoort op de peer-switch een vPC- of weespoort is, is niet van belang; het gaat erom dat het verkeer binnenkomt via de vPC-peer-link en bestemd is voor een vPC die op beide switches actief is. Om dit probleem te voorkomen, moet u ervoor zorgen dat de beheerstatus van de SVI's op beide switches consistent is en dat hun configuraties symmetrisch zijn.

Scenario 2: Alle vPC's en SVI's zijn omhoog - Next Hop Points to the vPC Peer

In dit scenario zijn alle SVI's en vPC-poortkanalen binnen het vPC-domein beschikbaar. N9K-C9504-5, dat via een Layer 3-interface is verbonden met N9K-C9364C-1, kan Loopback 0 echter niet pingen op N9K-C9364C-3.

Een traceroute van N9K-C9504-5 geeft aan dat het pakket eerst zijn directe volgende hop bereikt op 192.168.1.2 en vervolgens doorgaat naar 192.168.100.2, dat is gekoppeld aan N9K-C9364C-2.

```
N9K-C9504-5#
```

traceroute 172.16.100.10

```
traceroute to 172.16.100.10 (172.16.100.10), 30 hops max, 40 byte packets
1 192.168.1.2
```

(192.168.1.2)

```
 1.338 ms 0.912 ms 0.707 ms
2 192.168.100.2
```

(192.168.100.2)

```
 0.948 ms 0.751 ms 0.731 ms
3 * * *
4 * * *
N9K-C9504-5#
```

De volgende hopverificatie van N9K-C9364C-1 (de eerste hop voor dit verkeer) laat zien dat de bestemming bereikbaar is via 192.168.100.2, wat overeenkomt met SVI 100 op N9K-C9364C-2.

<#root>

```
N9K-C9364C-1#
```

show ip route 172.16.100.10

```
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

172.16.100.0/24, ubest/mbest: 1/0
*
```

via 192.168.100.2

```
, [1/0], 00:05:05, static
N9K-C9364C-1#
```

Een gekleurde ping (een ping met een opgegeven MTU-grootte) wordt gebruikt om het pad te traceren dat door dit verkeer wordt genomen:

<#root>

```
N9K-C9364C-1#
```

show interface e1/58 counters detailed all | i "1024 to|Eth" ; sh int port-channel 100 counters detailed

```
Ethernet1/58
52.
```

```
Rx Packets from 1024 to 1518 bytes: = 100 <<<----- Ingress Eth1/58


60. Tx Packets from 1024 to 1518 bytes: = 0
port-channel100
52. Rx Packets from 1024 to 1518 bytes: = 0
60.

Tx Packets from 1024 to 1518 bytes: = 100 <<<----- Egress po100 (vPC peer-link)


port-channel10
52. Rx Packets from 1024 to 1518 bytes: = 0
60. Tx Packets from 1024 to 1518 bytes: = 0
N9K-C9364C-1#
```

<#root>

```
N9K-C9364C-2# sh int port-channel 100 counters detailed all | i "1024 to|po" ; sh int port-channel 10 c
port-channel100
52.

Rx Packets from 1024 to 1518 bytes: = 100 <<<----- Ingress po100 (vPC peer-link)


60. Tx Packets from 1024 to 1518 bytes: = 0
port-channel10
52. Rx Packets from 1024 to 1518 bytes: = 0
60.

Tx Packets from 1024 to 1518 bytes: = 0 <<<----- Egress vPC po10, no packets!!!


N9K-C9364C-2#
```

Hoewel het verkeer op N9K-C9364C-2 aankomt via de vPC-peerlink, wordt het niet doorgestuurd naar vPC-poortkanaal 10. Dit komt omdat de egress_vsl_drop bit is ingesteld op 1 voor deze vPC, wat gebeurt wanneer hetzelfde vPC-poortkanaal in gebruik is op de peer-switch (in dit geval N9K-C9364C-1).

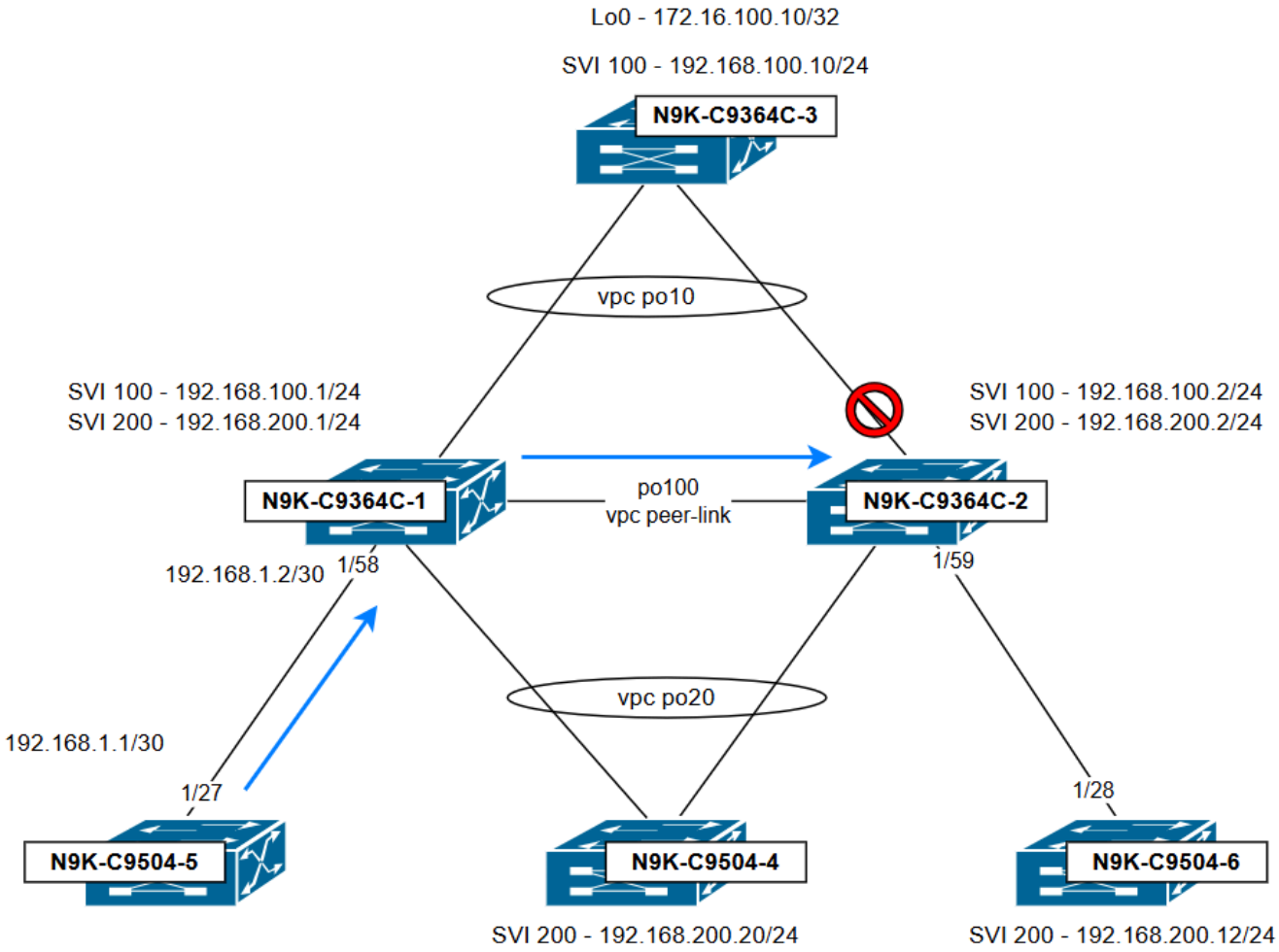
<#root>

```
N9K-C9364C-2#

show system internal eltm info interface Po10 | i i vsl


egress_vsl_drop = 1


N9K-C9364C-2#
```

<#root>

```
N9K-C9364C-2# show system internal vPCm info interface Po10 | i "Peer stat|Inform|vPC sta"
IF Elem Information:
MCECM DB Information:

vPC state: Up Old Compat Status: Pass


vPC Peer Information:

Peer state: Up <<<------------ vPC 10 up on peer


PSS Information:
vPC state: Up Old Compat Status: Pass
vPC Peer Information:

Peer state: Up <<<------------ vPC 10 up on peer


Shared Database Information:
Application database Information:
Lock Information:
N9K-C9364C-2#
```

Topologie die de verkeersstroom en het punt waarop deze wordt gedropt illustreert:



Conclusie:

Het probleem wordt waargenomen omdat N9K-C9364C-1 N9K-C9364C-2 gebruikt als de volgende hop, waarbij verkeer over de vPC-peer-link wordt verzonden voordat deze via vPC 10 probeert af te sluiten. Het verkeer is weggevallen vanwege de vermijdingsregel voor vPC-lus: verkeer dat via de vPC-peer-link wordt ontvangen, kan niet worden doorgestuurd naar een vPC-poortkanaal dat op beide switches actief is. Om dit probleem te voorkomen, moet u ervoor zorgen dat routes (dynamisch of statisch) met een volgende stap via een vPC-poortkanaal zijn geconfigureerd op beide vPC-peer-switches, zodat het verkeer niet over de vPC-peer-link hoeft te gaan en over een vPC hoeft te gaan.

Scenario 3: Alle vPC's en SVI's zijn ingeschakeld - VPC Peer-Gateway-functie is uitgeschakeld

In dit scenario staan alle SVI's en vPC-poortkanalen op het vPC-domein; de functie voor vPC peer-gateway is echter uitgeschakeld. Op dit moment kan N9K-C9504-4 (VLAN 200) N9K-C9364C-3 (VLAN 100) niet pingen.

```
<#root>

N9K-C9504-4#

ping 192.168.100.10


PING 192.168.100.10 (192.168.100.10): 56 data bytes
Request 0 timed out
Request 1 timed out
Request 2 timed out
Request 3 timed out
Request 4 timed out

--- 192.168.100.10 ping statistics ---

5 packets transmitted, 0 packets received, 100.00% packet loss


N9K-C9504-4#
```

De volgende hopverificatie van N9K-C9504-4 toont aan dat de bestemming bereikbaar is via 192.168.200.2, wat overeenkomt met SVI 200 op N9K-C9364C-2 en verbonden via vPC-poortkanaal 20.

```
<#root>

N9K-C9504-4#

show ip route 192.168.100.10


IP Route Table for VRF "default"
```

```
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

0.0.0.0/0, ubest/mbest: 1/0
*via
```

192.168.200.2

```
, [1/0], 01:22:46, static
N9K-C9504-4#
```

<#root>

N9K-C9504-4#

show ip arp detail | i 192.168.200.2

192.168.200.2

00:08:05

a478.06de.7edb

Vlan200 port-channel20 default

Een gekleurde ping (een ping met een opgegeven MTU-grootte) wordt gebruikt om het pad te traceren dat door dit verkeer wordt genomen. Hier onthullen de interfacetellers dat N9K-C9364C-1 het verkeer van 192.168.200.20 tot 192.168.100.10 ontvangt over poort-kanaal 20 en het naar de vPC peer-link (poort-kanaal100) verzendt

<#root>

N9K-C9364C-1#

show interface port-channel 20 counters detailed all | i "1024 to|po" ; sh int port-channel 10 counters

```
port-channel20
52.
```

Rx Packets from 1024 to 1518 bytes: = 100   <<<----- Ingress vPC 20

```
60. Tx Packets from 1024 to 1518 bytes: = 0
port-channel10
52. Rx Packets from 1024 to 1518 bytes: = 0
60. Tx Packets from 1024 to 1518 bytes: = 0
port-channel100
52. Rx Packets from 1024 to 1518 bytes: = 0
60.
```

Tx Packets from 1024 to 1518 bytes: = 100   <<<----- Egress po100 (vPC peer-link)

```
N9K-C9364C-1#
```

N9K-C9364C-2 ontvangt het verkeer via de vPC peer-link (port-channel100), maar stuurt het niet door naar vPC port-channel 10.

<#root>

```
N9K-C9364C-2#
```

show int port-channel 20 counters detailed all | i "1024 to|po" ; sh int port-channel 10 counters detail

```
port-channel20
52. Rx Packets from 1024 to 1518 bytes: = 0
60. Tx Packets from 1024 to 1518 bytes: = 0
port-channel10
52. Rx Packets from 1024 to 1518 bytes: = 0
60. Tx Packets from 1024 to 1518 bytes: = 0
```

<<<----- Egress vPC po10, no packets!!!

```
port-channel100
```

52. Rx Packets from 1024 to 1518 bytes: = 100 <<<----- Ingress po100 (vPC peer-link)

```
60. Tx Packets from 1024 to 1518 bytes: = 0
N9K-C9364C-2#
```

Hoewel het verkeer op N9K-C9364C-2 aankomt via de vPC-peerlink, wordt het niet doorgestuurd naar vPC-poortkanaal 10. Dit komt omdat de egress_vsl_drop bit is ingesteld op 1 voor deze vPC, wat gebeurt wanneer hetzelfde vPC-poortkanaal werkt op de peer-switch (in dit geval N9K-C9364C-1).

Aangezien peer-gateway is uitgeschakeld, kan N9K-C9364C-1 alleen pakketten routeren die zijn geadresseerd aan zijn eigen lokale MAC-adres. Als gevolg hiervan worden pakketten die bestemd zijn voor a478.06de.7edb (MAC van N9K-C9364C-2) doorgestuurd door N9K-C9364C-1 via de vPC peer-link.

<#root>

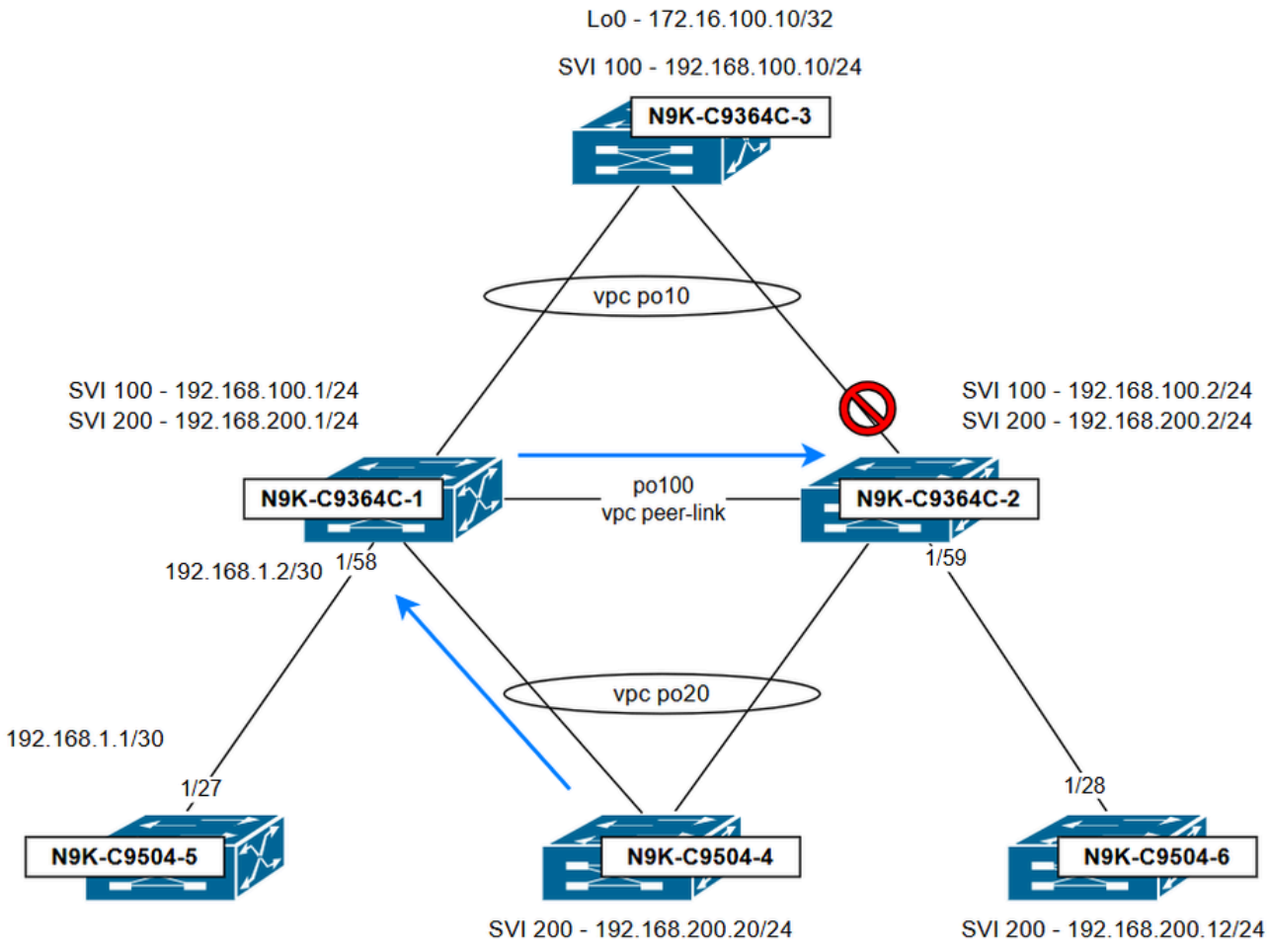
```
N9K-C9364C-1#
```

show mac address-table add a478.06de.7edb

```
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan
VLAN MAC Address Type age Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
* 100
```

```
a478.06de.7edb

 static - F F

vPC Peer-Link

(R)
* 200

a478.06de.7edb

 static - F F

vPC Peer-Link

(R)
N9K-C9364C-1#
```

Topologie die de verkeersstroom en het punt waarop deze wordt gedropt illustreert:



Conclusie:

Als peer-gateway is ingeschakeld, wordt het gerouteerde verkeer dat bestemd is voor het MAC-adres van de vPC-peer lokaal verwerkt door de peer-MAC als gateway te programmeren. Dit voorkomt dat de vPC-peer-link wordt gebruikt in het verkeerspad en voorkomt valpartijen

veroorzaakt door de vPC-lusvermijdingsregel. Om dergelijke problemen te voorkomen, moet u ervoor zorgen dat de functie vPC peer-gateway is ingeschakeld in het vPC-domein.

Overzicht van oplossing

- Houd de SVI-configuratie consistent op vPC VLAN's.

Asymmetric Switched Virtual Interface (SVI)-configuraties tussen vPC-peer-switches kunnen leiden tot problemen met het doorsturen van verkeer, waaronder het blokkeren van verkeer. Een veel voorkomende maar niet-ondersteunde praktijk die bijdraagt aan deze aandoening is het testen van failover tussen vPC-peers door SVI's aan één kant uit te schakelen. Deze methode creëert een asymmetrische SVI-status die de Nexus vPC-architectuur niet ondersteunt, wat resulteert in het blokkeren van verkeer en het doorsturen van fouten. Zorg ervoor dat de SVI-configuratie altijd consistent is op alle vPC-VLAN's waarvoor routering nodig is.

- Peer-gateway inschakelen in het vPC-domein.

De peer-gateway-functie is een belangrijke verbetering in Cisco Nexus vPC-implementaties. Wanneer deze optie is ingeschakeld in het vPC-domein, kan elke vPC-peer-switch pakketten accepteren en verwerken die bestemd zijn voor het virtuele MAC-adres van de vPC-peer. Dit betekent dat elke vPC-peer kan reageren op gateway-gebonden verkeer, ongeacht welke switch het pakket oorspronkelijk heeft ontvangen. Zonder peer-gateway ingeschakeld, kunnen bepaalde soorten verkeer, zoals pakketten die naar het standaard MAC-adres van de gateway worden verzonden, worden verwijderd als ze op één peer aankomen en anders de peer-link moeten doorlopen en een vPC-lidpoort moeten verlaten. Zorg ervoor dat vPC peer-gateway is geconfigureerd op het vPC-domein.

Gerelateerde informatie

Inzicht in verbeteringen in Virtual Port Channels (vPC)

Best practices voor Virtual Port Channels (vPC) op Nexus

Peer Gateway-functie op de Nexus 7000

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.